



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

76

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,794	12/28/2001	Keiichi Teramoto	217811US2RD	3076
22850	7590	04/26/2006	EXAMINER	
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.				SCHUBERT, KEVIN R
1940 DUKE STREET				
ALEXANDRIA, VA 22314				
ART UNIT		PAPER NUMBER		
2137				

DATE MAILED: 04/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/028,794	TERAMOTO ET AL.
	Examiner Kevin Schubert	Art Unit 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 12 April 2006.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1,2,10 and 11 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1,2,10,11 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date _____.
4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
5) Notice of Informal Patent Application (PTO-152)
6) Other: _____.

DETAILED ACTION

Claims 1-2 and 10-11 have been considered. Examiner maintains the rejections presented in the previous action.

5

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

10 (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

15

Claims 1-2 and 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,937,063, in view of Nagai, U.S. Patent No. 6,938,162.

20 As per claims 1 and 10, the applicant describes a method for sharing encrypted data region comprising the following limitations which are met by Davis and Nagai:

- a) giving a common key to each one of the two or more processes in advance (Davis: Col 3, lines 11-61);
- b) shifting an execution mode of the tamper resistant processor to an encrypted instruction execution mode (Davis: Col 3, lines 11-61);
- c) operating an owner process among the two or more processes to generate a shared encrypted data region valid only with respect to the common key in a process space of the owner process (Davis: Col 3, lines 11-61);
- d) operating each client process other than the owner process among the two or more processes to map the shared encrypted data region generated by the owner process to a process space of the each client process (Davis: Col 3, lines 11-61);

Art Unit: 2137

e) setting address information of the shared encrypted data region for each process among the two or more processes in relation to the common key in an encrypted attribute register inside the tamper resistant processor (Nagai: Col 15, lines 40-56).

Davis is silent as to setting address information in a register, as pertaining to part e of the claimed invention. Nagai discloses this limitation in a system which maintains an encrypted area management register in order to facilitate data management of an encrypted data region. Combining the ideas of Nagai with those of Davis allows for setting address information of the shared encrypted data region in an encrypted attribute register inside the tamper resistant processor. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Nagai with those of Davis because doing so makes the system more robust by facilitating data management of the encrypted data region.

As per claims 2 and 11, the applicant describes the method of claims 1 and 10, which are met by Davis in view of Nagai, with the following limitation which is also met by Davis in view of Nagai:

15 Encrypting/decrypting data to be sent/received to/from an external memory at the tamper resistant processor by referring to information set in the encrypted attribute register inside the tamper resistant processor when the each process carries out a write/read operation with respect to the shared encrypted data region (Davis: Col 3, lines 11-61; Nagai: Col 15, lines 40-56).

20 ***Response to Arguments***

Applicant has submitted that the objection to the Information Disclosure Statements raised in the previous action was improper because the submitted references were related cases, not requiring submission on a 1449 form. Examiner has withdrawn the objection and considered the related cases.

25 Applicant's arguments, see Remarks, filed 4/12/06, with respect to the 101 rejection of claims 1 and 2 have been fully considered and are persuasive. The 101 rejection has been withdrawn.

Art Unit: 2137

Applicant's arguments with respect to the 112, second paragraph, rejections of claims 1,2,10, and 11 have been fully considered and are persuasive. The 112 rejections have been withdrawn.

Applicant's arguments with respect to the 103(a) rejection of claim 1 et al under Davis in view of

5 Nagai have been fully considered, but they are not persuasive. Applicant presents the following argument:

1) Part d) is not met

Examiner respectfully disagrees. Specifically, Applicant argues that part d) is not met because
10 the host processor in the Davis reference "does not generate a data region valid only with respect to the shared secret key 64 in a process space of the host processor 50, and accordingly the secure boot device 54 does not map the data region generated by the host processor 50 to a process space of the secure boot device 54..." (Remarks, page 3 lines 21-24). To what extent the above statements are true, Examiner notes that the instant rejection does not depend on the contrary. Examiner further submits that
15 Applicant may have mischaracterized the instant rejection.

Davis discloses that a secure boot device may maintain an encrypted data region, comprising data such as an encrypted boot-up instruction (e.g. Col 3, lines 32-34). The encrypted data region is shared between the secure boot device and a host processor. Processes associated with a host processor request an encrypted boot-up instruction, receive an encrypted boot-up instruction, and map an
20 encrypted boot-up instruction to a process space of a host processor (e.g. Col 3, lines 34-36). Further, the host processor may decrypt the encrypted boot-up instruction using a shared secret key (e.g. Col 3, lines 36-39). Accordingly, Examiner submits that Davis discloses part d) of claim 1, and the rejection is maintained.

25

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2137

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action 5 is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally 10 be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application 15 Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

20

KS



EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER